EXHIBIT F

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al.	)	
	)	
Plaintiffs,	)	
	)	
v.	)	CIVIL ACTION
	)	FILE NO.:
BRIAN P. KEMP, in his individual capacity and his official capacity as Secretary of State of Georgia and Chair of the STATE ELECTION BOARD, et al.,	)	
	)	
Defendants.	)	

AFFIDAVIT OF EDWARD W. FELTEN

EDWARD W. FELTEN ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the Director of Princeton's Center for Information Technology Policy. I received my Ph.D. in Computer Science and Engineering from the University of Washington in 1993. I am a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

2. From 2015 until January 2017, I served in the White House as Deputy United States Chief Technology Officer. During that time I advised the President and his senior advisors on policy issues relating to computer science, including issues relating to the security and reliability of elections and electronic voting systems.

3. A copy of my curriculum vitae is attached as Exhibit A.

Inherent risks of paperless electronic voting machines

4. Before turning to the systems and circumstances specific to Georgia elections, I will provide a brief summary of cybersecurity issues relating to voting machines.

5. The voting machines at issue are a type of so-called Direct Recording Electronic (DRE) machine. DREs are voting machines that are designed to record a voter's ballot directly in electronic storage, without creating any record of the ballot that can be directly verified by the voter.

6. DREs can be contrasted with other voting technologies in which there is a record of the voter's ballot, typically on paper, the accuracy of which can be verified directly by the voter in the polling place, and which is collected at the polling place as a record of the voter's intent. The most common examples of voter-verifiable ballots include paper ballots. Paper ballots can be tabulated by hand counting. Alternatively, they can be tabulated securely by a machine such as an optical scanner, provided that a post-election audit is performed to confirm that the machine count is consistent with the results of manually inspecting a suitable sample of paper ballots.

7. The lack of a voter-verifiable ballot creates special risks associated with any DRE voting system. For this reason, computer scientists and cybersecurity experts typically recommend against the use of DREs. I concur with this general recommendation against the use of DREs.

8. The hardware of a DRE—the physical equipment comprising the computer—is much like a standard desktop computer, often installed into a different physical enclosure. Like a standard computer, a DRE will do whatever the software installed in it directs it to do. If anyone changes the software, whether through malice or error, the DRE may do something other than accurately recording and tabulating votes.

9. A malicious modification to a DRE's software would likely cause the DRE to modify ballots silently. The modified software could be designed to report on the machine's display screen, to voters and election officials, that all was well. It could also be designed to falsify all of the logs and records kept by the voting machine.

10. My students and I have modified the software on many types of DREs. For example, my students modified a (now decommissioned) New York DRE to turn it into a kiosk for playing the popular arcade game Pac-Man. We have also created, installed, and tested software for multiple DRE models that would silently modify election results. (For obvious reasons, these latter tests were done in secure laboratories.)

My team's study of Diebold voting machines

11. I led a team of researchers that studied the Diebold AccuVote TS voting machine system. We published a peer-reviewed paper summarizing our analysis, which is attached as Exhibit B.

12. As part of our research we demonstrated that it was possible to create a voting machine virus: a computer virus that infected the voting machines, spreading from machine to machine by infecting the memory cards that are used to transport election and ballot information between the machines and central tabulation offices. The virus, having infected a voting machine, would modify election results, without leaving any trace in the logs or records kept by the machine. We created and tested such a virus in our secure laboratory.

13. The voting machine virus we created could spread from machine to machine even though the machines were never connected to any network. The virus would spread by infecting memory cards that were transported between machines. When a memory card was inserted into an infected machine, the virus would infect the memory card. When an infected memory card was inserted into a previously unaffected machine, the virus would infect this machine. Thus the memory cards acted as carriers for the virus, much as mosquitoes act as carriers for some human diseases.

14. The notion that machines not connected to the Internet are somehow immune to viruses or other security compromise is a fallacy. It is inconsistent with decades of experience with cybersecurity. In the specific case of Georgia voting machines, it is directly disproven by the research in my laboratory.

15. I did a live demonstration of this election-stealing virus, including showing the casting of votes and mis-reporting of the vote counts by the machine, during live testimony at a hearing of a committee of the U.S. House of Representatives. My students and I did a similar demonstration twice on live television, on CNN and Fox News.

16. The TS machine we studied allowed modified (and possibly malicious) software to be installed by anyone who could open a small metal access door on the side of the machine. The door was locked by an ordinary file cabinet type of lock. Because the very same key that is used for the access door on the AccuVote TS is also used widely on office furniture, jukeboxes, and hotel minibars, the keys are easily purchased. I bought a gross of these keys (i.e., 144 keys) from a vendor on the Internet. The lock is also easily picked—a member of our team who studies locks as hobby was able to pick the access door lock consistently in less than 15 seconds.

17. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes.

18. Our peer reviewed paper listed a number of other security problems with the AccuVote TS system. Some of these problems could in principle be fixable by improving the software of the TS, but others are inherent in the machine's hardware and therefore not fixable by any software update.

19. As described in our peer reviewed paper, it is inherent in the hardware design of the TS that a person who can get physical access to the inside of the machine can install any software they like on the machine.

20. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes. This problem is inherent in the hardware design of the TS machine.

21. Subsequent to the publication of our paper, we studied the AccuVote TSX system and found that it had similar security problems.

Need for software verification

22. One cannot know that any DRE machine, including a TS or TSX, will accurately record or tabulate votes, unless one is certain as to which software is installed on that machine. Because of the ease of malicious modification of the software, it is not enough to know which software is supposed to be installed—one must inspect the machine to verify which software is actually installed.

23. Verifying which software is actually installed is technically very difficult, because one cannot rely on the software itself to report its own status accurately. Malicious software can simply misreport its own status, reporting that everything is normal. Relying on the software to report whether it has been tampered with is like trying to determine whether a person is honest by asking him, "Are you honest?" An answer of "yes" is not reliable evidence.

24. Unfortunately, the standard methods for inspecting the software version installed in a machine rely on the machine's software in one way or another, so they fail to avoid this pitfall and should not be trusted. Special protocols, typically involving the use of specialized equipment, must be designed and used to perform such inspections, and rigorous chain-of-custody controls are necessary after the inspection to make sure no tampering with the machine's software could have occurred after the inspection.

25. Unless all of these steps are followed, with respect to a particular DRE machine, one cannot be confident in its ability to accurately record or tabulate votes.

Need for secure facilities

26. I understand that Georgia voting machines are tested and configured in the Center for Election Systems (CES) at Kennesaw State University (KSU). Because my team's research has demonstrated the propagation of malicious software during these types of activities, including propagation to systems not directly connected to the Internet, any security breach at CES, or failure to implement adequate cybersecurity precautions at CES, could have created an opportunity for a malicious party to modify software in voting machines and related systems.

27. The security breach at CES, and KSU's response to it, are indications that cybersecurity precautions at CES may not have been adequate. It is significant that KSU's response to the breach included steps to change how cybersecurity and system administration were managed at CES, so that CES personnel were no longer managing these functions on their own. It is significant that the post-breach report from KSU's Information Security Office listed as its first "Opportunit[y] for Improvement" the "Poor understanding of risk posed by [CES] IT systems."

28. The most sophisticated cyberattackers are especially skilled not only at gaining unauthorized access to systems, but also at maintaining access. So-called Advanced Persistent Threat actors specialize in gaining access and maintaining that access over time, while avoiding detection and waiting for the best moment to strike. Once they are in a system, it can be extraordinarily difficult to find them. As a result, very stringent measures may be necessary to

render a facility safe after a period of vulnerability—and especially when highly skilled actors may have been motivated to compromise that facility.

29. Because of the vulnerability of the DRE voting machines to software manipulation, and because of intelligence reports about highly skilled cyber-actors having attempted to affect elections in the United States, such precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism.

30. Further Affiant sayeth not.

Edward W. Felten

State of New Jersey
County of Mercer

Taylor J Cerverizzo, Notary Public

TAYLOR J CERVERIZZO
Comm. Exp. September 3, 2020
NOTARY
PUBLIC
Comm. #50022638
NEW JERSEY

Edward W. Felten

Education

Ph.D. in Computer Science and Engineering, University of Washington, 1993.
Dissertation title: "Protocol Compilation: High-Performance Communication for Parallel Programs." Advisors: Edward D. Lazowska and John Zahorjan.
M.S. in Computer Science and Engineering, University of Washington, 1991.
B.S. in Physics, with Honors, California Institute of Technology, 1985.

Employment

Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University, 2013-present

Deputy United States Chief Technology Officer, The White House, Office of Science and Technology Policy, 2015-2017

Professor of Computer Science and Public Affairs, Princeton University, 2006-2013.

Chief Technologist, U.S. Federal Trade Commission, 2011-2012.

Professor of Computer Science, Princeton University, 2003-2006.
Associate Professor of Computer Science, Princeton University, 1999-2003.
Assistant Professor of Computer Science, Princeton University, 1993-99.
Senior Computing Analyst, Caltech Concurrent Computing Project, California Institute of Technology, 1986-1989.

Director, Center for Information Technology Policy, Princeton University, 2005-present.

Elysium Digital LLC and various law firms. Consulting and expert testimony in technology litigation, 1998-2015
U.S. Federal Trade Commission: consulting regarding spam policy and investigation, 2004, 2006.
U.S. Dept. of Justice, Antitrust Division: consulting and testimony in Microsoft antitrust case, 1998-2002..
Electronic Frontier Foundation. Consulting in intellectual property / free speech lawsuits, 2001-2010.
Certus Ltd.: consultant in product design and analysis, 2000-2002.
Cigital Inc.: Technical Advisory Board member, 2000-2007.
Cloakware Ltd.: Technical Advisory Board member, 2000-2003.
Propel.com: Technical Advisory Board member, 2000-2002.

NetCertainty.com: Technical Advisory Board member, 1999-2002.
FullComm LLC: Scientific Advisory Board member, 1999-2001.
Sun Microsystems: Java Security Advisory Board member, 1997-2001.
Finjan Software: Technical Advisory Board member, 1997-2002.
International Creative Technologies: consultant in product design and analysis, 1997-98.
Bell Communications Research: consultant in computer security research, 1996-97.

Honors and Awards

National Academy of Engineering, 2013.
Alumni Achievement Award, University of Washington, 2013.
American Academy of Arts and Sciences, 2011.
E-Council Teaching Award, School of Engineering and Appl. Sci., Princeton, 2010.
ACM Fellow, 2007.
EFF Pioneer Award, 2005.
Scientific American Fifty Award, 2003.
Alfred P. Sloan Fellowship, 1997.
Emerson Electric, E. Lawrence Keyes Faculty Advancement Award, Princeton University School of Engineering, 1996.
NSF National Young Investigator award, 1994.
Outstanding Paper award, 1997 Symposium on Operating Systems Principles.
Best Paper award, 1995 ACM SIGMETRICS Conference.
AT&T Ph.D. Fellowship, 1991-93.
Mercury Seven Foundation Fellowship, 1991-93.

Research Interests

Information security. Privacy. Technology law and policy. Internet software. Intellectual property policy. Using technology to improve government. Operating systems. Distributed computing. Parallel computing architecture and software.

Professional Service

Professional Societies and Advisory Groups

ACM U.S. Public Policy Council, Chair, 2014-2015.
ACM U.S. Public Policy Committee, Vice Chair, 2008-2010, 2012-2014.
DARPA Privacy Panel, 2010-2012.
Transportation Security Administration, Secure Flight Privacy Working Group, 2005.
National Academies study committee on Air Force Information Science and Technology Research, 2004.
Electronic Frontier Foundation, Advisory Board, 2004-2007.
ACM U.S. Public Policy Committee, 2004-present (Executive Committee, 2005-present)

ACM Advisory Committee on Security and Privacy, 2002-2003.
DARPA Information Science and Technology (ISAT) study group, 2002-2004.
Co-chair, ISAT study committee on "Reconciling Security with Privacy," 2001-2002.
National Academy study committee on Foundations of Computer Science, 2001-2004.

Program Committees

World Wide Web Conference, 2006.
USENIX General Conference, 2004.
Workshop on Foundations of Computer Security, 2003.
ACM Workshop on Digital Rights Management, 2001.
ACM Conference on Computer and Communications Security, 2001.
ACM Conference on Electronic Commerce, 2001.
Workshop on Security and Privacy in Digital Rights Management, 2001.
Internet Society Symposium on Network and Distributed System Security, 2001.
IEEE Symposium on Security and Privacy, 2000.
USENIX Technical Conference, 2000.
USENIX Windows Systems Conference, 2000.
Internet Society Symposium on Network and Distributed System Security, 2000.
IEEE Symposium on Security and Privacy, 1998.
ACM Conference on Computer and Communications Security, 1998.
USENIX Security Symposium, 1998.
USENIX Technical Conference, 1998.
Symposium on Operating Systems Design and Implementation, 1996.

Boards

Verified Voting, Advisory Board, 2013-present.
Electronic Privacy Information Center, Advisory Board, 2013-present.
Electronic Frontier Foundation, Board of Directors, 2007-2010.
DARPA Information Science and Technology study board, 2001-2003.
Cigital Inc.: Technical Advisory Board (past).
Sun Microsystems, Java Security Advisory Council (past).
Cloakware Ltd.: Technical Advisory Board (past).
Propel.com: Technical Advisory Board (past).
Finjan Software: Technical Advisory Board (past).
Netcertainty: Technical Advisory Board (past).
FullComm LLC: Scientific Advisory Board (past).

University and Departmental Service

Council on Teaching and Learning, 2014-2015.
School of Engineering and Appl. Sci., Strategic Plan Steering Committee, 2014-2015
Committee on Online Courses, 2012-2013.
Director, Center for Information Technology Policy, 2005-present.
Committee on the Course of Study, 2009-present.
SEAS Strategic Planning, 2004.
    Member, Executive Committee
    Co-Chair, Interactions with Industry area.

Co-Chair, Engineering, Policy, and Society area.

Faculty Advisory Committee on Policy, 2002-present.

Council of the Princeton University Community, 2002-present (Executive Committee)

Faculty Advisory Committee on Athletics, 1998-2000.

Computer Science Academic Advisor, B.S.E. program, class of 1998 (approx. 25 students)

Faculty-Student Committee on Discipline, 1996-98.

Faculty-Student Committee on Discipline, Subcommittee on Sexual Assault and Harrassment, 1996-98.

Students Advised

Ph.D. Advisees:

Harlan Yu (Ph.D. 2012). Dissertation: Designing Software to Shape Open Government Policy. Founder, Upturn Partners.

Ariel J. Feldman (Ph.D. 2012). Dissertation: Privacy and Integrity in the Untrusted Cloud. Assistant Professor of Computer Science, University of Chicago.

Joseph A. Calandrino (Ph.D. 2012). Dissertation: Control of Sensitive Data in Systems with Novel Functionality. Consulting Computer Scientist, Elysium Digital.

William B. Clarkson (Ph.D. 2012). Dissertation: Breaking Assumptions: Distinguishing Between Seemingly Identical Items Using Cheap Sensors. Technical staff member at Google.

Matthias Jacob (Ph.D. 2009). Technical staff member at Nokia.

J. Alex Halderman (Ph.D. 2009). Dissertation: Security Failures in Non-traditional Computing Environments. Associate Professor of Computer Science, University of Michigan.

Shirley Gaw (Ph.D. 2009). Dissertation: Ideals and Reality: Adopting Secure Technologies and Developing Secure Habits to Prevent Message Disclosure. Technical staff member at Google.

Brent Waters (Ph.D. 2004). Dissertation: Security in a World of Ubiquitous Recording Devices. Professor of Computer Science, University of Texas.

Robert A. Shillingsburg (Ph.D. 2004). Dissertation: Improving Distributed File Systems using a Shared Logical Disk. Retired; previously a technical staff member at Google.

Michael Schneider (Ph.D. 2004). Dissertation: Network Defenses against Denial of Service Attacks. Researcher, Supercomputing Research Center, Institute for Defense Analyses.

Minwen Ji (Ph.D. 2001). Dissertation: Data Distribution for Dynamic Web Content. Researcher, HP Labs.

Dirk Balfanz (Ph.D. 2000). Dissertation: Access Control for Ad Hoc Collaboration. Technical staff member at Google.

Dan S. Wallach (Ph.D. 1998). Dissertation: A New Approach to Mobile Code Security. Professor of Computer Science, Rice University.

Significant Advisory Role:

Drew Dean (Ph.D. 1998). Advisor: Andrew Appel. Research Scientist, SRI International.

Stefanos Damianakis (Ph.D. 1998). Advisor: Kai Li. President and CEO, Netrics, Inc.

Pei Cao (Ph.D. 1996). Advisor: Kai Li. Technical staff at Facebook.

Lujo Bauer (Ph.D. 2003). Advisor: Andrew Appel. Associate Professor, School of Computer Science, Carnegie Mellon University.

Publications

Books and Book Chapters

[1] The Economics of Bitcoin, or Bitcoin in the Presence of Adversaries. Joshua A. Kroll, Ian Davey, and Edward W. Felten. To appear, Lecture Notes in Computer Science series.

[2] Enabling Innovation for Civic Engagement. David G. Robinson, Harlan Yu, and Edward W. Felten. In Open Government, Daniel Lathrop and Laurel Ruma, eds., O'Reilly, 2010.

[3] Securing Java: Getting Down to Business with Mobile Code. Gary McGraw and Edward W. Felten. John Wiley and Sons, New York 1999.

[4] Java Security: Web Browsers and Beyond. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz. In "Internet Besieged: Countering Cyberspace Scofflaws," Dorothy E. Denning and Peter J. Denning, eds. ACM Press, New York, 1997.

[5] Java Security: Hostile Applets, Holes and Antidotes. Gary McGraw and Edward Felten. John Wiley and Sons, New York, 1996

[6] Dynamic Tree Searching. Steve W. Otto and Edward W. Felten. In "High Performance Computing", Gary W. Sabot, ed., Addison Wesley, 1995.

Journal Articles

[7] Accountable Algorithms. Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. University of Pennsylvania Law Review, Vol. 165, 2017. *Forthcoming. 2016 Future of Privacy Forum Privacy Papers for Policymakers Award.*

[8] Government Data and the Invisible Hand. David Robinson, Harlan Yu, William Zeller, and Edward W. Felten. Yale Journal of Law and Technology, vol. 11, 2009.

[9] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Software – Practice and Experience, 33:461-480, 2003.

[10] The Digital Millennium Copyright Act and its Legacy: A View from the Trenches. Illinois Journal of Law, Technology and Policy, Fall 2002.

[11] The Security Architecture Formerly Known as Stack Inspection: A Security Mechanism for Language-based Systems. Dan S. Wallach, Edward W. Felten, and Andrew W. Appel. ACM Transactions on Software Engineering and Methodology, 9:4, October 2000.

[12] Statically Scanning Java Code: Finding Security Vulnerabilities. John Viega, Tom Mutdosch, Gary McGraw, and Edward W. Felten. IEEE Software, 17(5), Sept./Oct. 2000.

[13] Client-Server Computing on the SHRIMP Multicomputer. Stefanos N. Damianakis, Angelos Bilas, Cezary Dubnicki, and Edward W. Felten. IEEE Micro 17(1):8-18, February 1997.

[14] Fast RPC on the SHRIMP Virtual Memory Mapped Network Interface. Angelos Bilas and Edward W. Felten. IEEE Transactions on Parallel and Distributed Computing, February 1997.

[15] Implementation and Performance of Integrated Application-Controlled File Caching, Prefetching and Disk Scheduling. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. ACM Transactions on Computer Systems, Nov 1996.

[16] Virtual Memory Mapped Network Interface Designs. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, Kai Li, and Malena Mesarina. IEEE Micro, 15(1):21-28, February 1995.

Selected Symposium Articles

[17] Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. IEEE Symposium on Security and Privacy, 2015.

[18] A Precautionary Approach to Big Data Privacy. Edward W. Felten, Joanna Huey, and Arvind Narayanan. Conference on Privacy and Data Protection, 2015.

[19] On Decentralizing Prediction Markets and Order Books. Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Mill, and Arvind Narayanan. Workshop on Economics of Information Security, May 2014.

[20] Mixcoin: Anonymity for Bitcoin with Accountable Mixes. Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. Proceedings of Financial Cryptography, February 2014.

[21] Privacy Concerns of Implicit Security Factors for Web Authentication. Joseph Bonneau, Edward W. Felten, Prateek Mittal, and Arvind Narayanan. Adventures in Authentication: WAY Workshop, 2014.

[22] The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Joshua Kroll, Ian Davey, and Edward W. Felten. Workshop on the Economics of Information Security, 2013.

[23] Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2012.

[24] Bubble Trouble: Off-Line De-Anonymization of Bubble Forms. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2011

[25] You Might Also Like: Privacy Risks of Collaborative Filtering. Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov. Proc. IEEE Symposium on Security and Privacy, May 2011.

[26] SPORC: Group Collaboration Using Untrusted Cloud Resources. Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. Proc. Symposium on Operating Systems Design and Implementation, 2010.

[27] SVC: Selector-Based View Composition for Web Frameworks. William Zeller and Edward W. Felten. Proc. USENIX Conference on Web Application Development, 2010.

[28] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmet Witchel. Proc. 17th Network and Distributed System Security Symposium, 2010.

[29] Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham, Proc. Electronic Voting Technology Workshop, 2009.

[30] Some Consequences of Paper Fingerprinting for Elections. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2009.

[31] Software Support for Software-Independent Auditing. Gabrielle A. Gianelli, Jennifer D. King, Edward W. Felten, and William P. Zeller. Proc. Electronic Voting Technology Workshop, 2009.

[32] Fingerprinting Blank Paper Using Commodity Scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Proc. ACM Symposium on Security and Privacy, May 2009.

[33] Lest We Remember: Cold Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Proc. Usenix Security Symposium, 2008.

[34] In Defense of Pseudorandom Sample Selection. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2008.

[35] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.

[36] Machine-Assisted Election Auditing. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.

[37] Lessons from the Sony CD DRM Episode. J. Alex Halderman and Edward W. Felten. Proc. Usenix Security Symposium, 2006.

[38] A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. Proc. 14th World Wide Web Conference, 2005.

[39] New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent R. Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. ACM Conference on Computer and Communications Security. November 2004.

[40] Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. 3rd Workshop on Privacy in Electronic Society. November 2004.

[41] Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Edward W. Felten, and Amit Sahai. ACM Conference on Computer and Communications Security. November 2003.

[42] Attacking an Obfuscated Cipher by Injecting Faults. Matthias Jacob, Dan Boneh, and Edward W. Felten. ACM Workshop on Digital Rights Management, November 2002.

[43] A General and Flexible Access-Control System for the Web. Lujo Bauer, Michael A. Schneider, and Edward W. Felten. 11th USENIX Security Symposium, August 2002.

[44] Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Batya Friedman, Daniel C. Howe, and Edward W. Felten. Hawaii International Conference on System Sciences, January 2002. (Best Paper award, organizational systems track.)

[45] Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, John P. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. USENIX Security Symposium, August 2001.

[46] Cookies and Web Browser Design: Toward Realizing Informed Consent Online. Lynette I. Millett, Batya Friedman, and Edward W. Felten. Proc. of CHI 2001 Conference on Human Factors in Computing Systems, April 2001.

[47] Timing Attacks on Web Privacy. Edward W. Felten and Michael A. Schneider. Proc. of 7th ACM Conference on Computer and Communications Security, Nov. 2000.

[48] Archipelago: An Island-Based File System for Highly Available and Scalable Internet Services. USENIX Windows Systems Symposium, August 2000.

[49] Proof-Carrying Authentication. Andrew W. Appel and Edward W. Felten. Proc. of 6th ACM Conference on Computer and Communications Security, Nov. 1999.

[50] An Empirical Study of the SHRIMP System. Matthias A. Blumrich, Richard D. Alpert, Yuqun Chen, Douglas W. Clark, Stefanos, N. Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, Margaret Martonosi, Robert A. Shillner, and Kai Li. Proc. of 25th International Symposium on Computer Architecture, June 1998.

[51] Performance Measurements for Multithreaded Programs. Minwen Ji, Edward W. Felten, and Kai Li. Proc. of 1998 SIGMETRICS Conference, June 1998.

[52] Understanding Java Stack Inspection. Dan S. Wallach and Edward W. Felten. Proc. of 1998 IEEE Symposium on Security and Privacy, May 1998.

[53] Extensible Security Architectures for Java. Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Proc. of 16th ACM Symposium on Operating Systems Principles, Oct. 1997. Outstanding Paper Award.

[54] Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Proc. of 20th National Information Systems Security Conference, Oct. 1997.

[55] Reducing Waiting Costs in User-Level Communication. Stefanos N. Damianakis, Yuqun Chen, and Edward W. Felten. Proc. of 11th Intl. Parallel Processing Symposium, April 1997.

[56] Stream Sockets on SHRIMP. Stefanos N. Damianakis, Cezary Dubnicki, and Edward W. Felten. Proc. of 1st Intl. Workshop on Communication and Architectural Support for Network-Based Parallel Computing, February 1997. (Proceedings available as Lecture Notes in Computer Science #1199.)

[57] Early Experience with Message-Passing on the SHRIMP Multicomputer. Richard D. Alpert, Angelos Bilas, Matthias A. Blumrich, Douglas W. Clark, Stefanos Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, and Kai Li. Proc. of 23rd Intl. Symposium on Computer Architecture, 1996.

[58] A Trace-Driven Comparison of Algorithms for Parallel Prefetching and Caching. Tracy Kimbrel, Andrew Tomkins, R. Hugo Patterson, Brian N. Bershad, Pei Cao, Edward W. Felten, Garth A. Gibson, Anna R. Karlin, and Kai Li. Proc. of 1996 Symposium on Operating Systems Design and Implementation.

[59] Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten, and Dan S. Wallach. Proc. of 1996 IEEE Symposium on Security and Privacy.

[60] Integrated Parallel Prefetching and Caching. Tracy Kimbrel, Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1996 SIGMETRICS Conference.

[61] Software Support for Virtual Memory-Mapped Communication. Cezary Dubnicki, Liviu Iftode, Edward W. Felten, and Kai Li. Proc. of Intl. Parallel Processing Symposium, April 1996.

[62] Protected, User-Level DMA for the SHRIMP Network Interface. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996

[63] Improving Release-Consistent Shared Virtual Memory using Automatic Update . Liviu Iftode, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996

[64] Synchronization for a Multi-Port Frame Buffer on a Mesh-Connected Multicomputer. Bin Wei, Gordon Stoll, Douglas W. Clark, Edward W. Felten, and Kai Li. Parallel Rendering Symposium, Oct. 1995.

[65] A Study of Integrated Prefetching and Caching Strategies. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1995 ACM SIGMETRICS Conference. Best Paper award.

[66] Evaluating Multi-Port Frame Buffer Designs for a Mesh-Connected Multicomputer. Gordon Stoll, Bin Wei, Douglas W. Clark, Edward W. Felten, Kai Li, and Patrick Hanrahan. Proc. of 22nd Intl. Symposium on Computer Architecture.

[67] Implementation and Performance of Application-Controlled File Caching. Pei Cao, Edward W. Felten, and Kai Li. Proc. of 1st Symposium on Operating Systems Design and Implementation, pages 165-178, November 1994.

[68] Application-Controlled File Caching Policies. Pei Cao, Edward W. Felten, and Kai Li. Proc. of USENIX Summer 1994 Technical Conference, pages 171-182, 1994.

[69] Virtual Memory Mapped Network Interface for the SHRIMP Multicomputer. Matthias A. Blumrich, Kai Li, Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Jonathan S. Sandberg. Proc. of Intl. Symposium on Computer Architecture, 1994.

[70] Performance Issues in Non-Blocking Synchronization on Shared-Memory Multiprocessors. Juan Alemany and Edward W. Felten. Proceedings of Symposium on Principles of Distributed Computing, 1992.

[71] Improving the Performance of Message-Passing Applications by Multithreading. Edward W. Felten and Dylan McNamee. Proceedings of Scalable High-Performance Computing Conference (SHPCC), 1992.

[72] A Highly Parallel Chess Program. Edward W. Felten and Steve W. Otto. 1988 Conference on Fifth Generation Computer Systems.

Selected Other Publications

[73] Testimony for Privacy and Civil Liberties Oversight Board hearing on "Defining Privacy". November 2014. Written testimony submitted December 2014.

[74] Heartbleed Shows Government Must Lead on Internet Security. Edward W. Felten and Joshua Kroll. *Scientific American*, July 2014.

[75] How the NSA Piggy-Backs on Third-Party Trackers. Edward Felten and Jonathan Mayer. Slate, Dec. 13, 2013.

[76] Testimony for Senate Judiciary Committee hearing on "Continued Oversight of the Foreign Intelligence Surveillance Act," October 2, 2013.

[77] The Chilling Effects of the DMCA. Edward Felten. *Slate*, March 29, 2013.

[78] CALEA II: Risks of Wiretap Modifications to Endpoints. [20 authors]. Submitted to a White House working group.

[79] Strangers in a Strange Land. Review of *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*, by Abelson, Ledeen, and Lewis. American Scientist, 97:4. July/August 2009.

[80] Lest We Remember: Cold-Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Communications of the ACM*, 52(5):91-98. May 2009.

[81] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Sept. 2006.

[82] Digital Rights Management, Spyware, and Security. Edward W. Felten and J. Alex Halderman, *IEEE Security and Privacy,* Jan./Feb. 2006.

[83] Inside RISKS: DRM and Public Policy. Edward W. Felten. Communications of the ACM, 48:7, July 2005.

[84] Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks? Edward W. Felten. IEEE Security and Privacy, May 2003.

[85] A Skeptical View of DRM and Fair Use. Edward W. Felten. Communications of the ACM 46(4):56-61, April 2003.

[86] Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace. Testimony before U.S. Senate Commerce Committee. September 2003.

[87] Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. Submitted for publication, 2003.

[88] An Efficient Heuristic for Defense Against Distributed Denial of Service Attacks using Route-Based Distributed Packet Filtering. Michael A. Schneider and Edward W. Felten. Submitted for publication, 2003.

[89] Written testimony to House Commerce Committee, Subcommittee on Courts, the Internet, and Intellectual Property, oversight hearing on "Piracy of Intellectual Property on Peer to Peer Networks." September 2002.

[90] Written testimony to Senate Judiciary Committee hearings on "Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creativity?" March 2002.

[91] Informed Consent Online: A Conceptual Model and Design Principles. Batya Friedman, Edward W. Felten, and Lynette I. Millett. Technical Report 2000-12-2, Dept. of Computer Science and Engineering, University of Washington, Dec. 2000.

[92] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Technical Report CS-TR-603-99, Department of Computer Science, Princeton University, July 1999.

[93] A Java Filter. Dirk Balfanz and Edward W. Felten. Technical Report 567-97, Dept. of Computer Science, Princeton University, October 1997.

[94] Inside RISKS: Webware Security. Edward W. Felten. Communications of the ACM, 40(4):130, 1997.

[95] Simplifying Distributed File Systems Using a Shared Logical Disk.Robert A. Shillner and Edward W. Felten. Princeton University technical report TR-524-96.

[96] Contention and Queueing in an Experimental Multicomputer: Analytical and Simulation-based Results. Wenjia Fang, Edward W. Felten, and Margaret Martonosi. Princeton University technical report TR-508-96.

[97] Design and Implementation of NX Message Passing Using SHRIMP Virtual Memory Mapped Communication. Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Kai Li. Princeton University technical report TR-507-96.

[98] Protocol Compilation: High-Performance Communication for Parallel Programs. Edward W. Felten. Ph.D. dissertation, Dept. of Computer Science and Engineering, University of Washington, August 1993.

[99] Building Counting Networks from Larger Balancers. Edward W. Felten, Anthony LaMarca, and Richard Ladner. Univ. of Washington technical report UW-CSE-93-04-09.

[100] The Case for Application-Specific Communication Protocols. Edward W. Felten. Univ. of Washington technical report TR-92-03-11.

[101] A Centralized Token-Based Algorithm for Distributed Mutual Exclusion. Edward W. Felten and Michael Rabinovich. Univ. of Washington technical report TR-92-02-02.

[102] Issues in the Implementation of a Remote Memory Paging System. Edward W. Felten and John Zahorjan. Univ. of Washington technical report TR-91-03-09.

EXHIBIT G

AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of the petition to void the June 20, 2017, election and to prohibit further use of Georgia's current DRE voting system..

2. In my opinion, the Diebold electronic voting system used in Georgia is vulnerable both to malicious interference and inadvertent error. The Diebold system in general has been put under technical scrutiny several times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has been successful.

3. The possible stamp of approval (for a modified system?) given by the Kennesaw State University (KSU) Center for Election Systems (CES) does not in my opinion mitigate for use in Georgia the known flaws of the system. Indeed, the recent reports from the Kim Zetter article for *Politico* seem to demonstrate that the KSU CES has been either unable or unwilling to address security, privacy, and integrity issues even when they have been privately disclosed to the CES by credible cybersecurity professionals. The fact that the FOIA request of Mr. Garland Favorito yielded only three emails between CES and Mr. Logan Lamb and Mr. Christopher Grayson suggests further that CES might not have been taking seriously the security threats that were pointed out by Lamb and Grayson.

Qualifications and Relevant Employment History

4. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell.

5. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

6. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics

different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the U.S. intelligence community.

7. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

8. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

9. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued. When

the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well. I have obtained and analyzed the data from the 2012, 2014, and 2016 elections in South Carolina, and I have also analyzed ES&S DRE-voting system data in more limited quantities from Colorado, North Carolina, Pennsylvania, and Texas.

Basis for My Opinions

10. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

11. I have also used for my opinions a review of the documents surrounding the KSU CES hack in Spring 2017, including the report attached to an email on 24 April 2017 from Stephen Gay to Merle King.

The Diebold Election System Was Unacceptable for Use in the CD6 Election Held 20 June 2017

12. I begin with the fact that the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems. The letter from Georgia citizens to Secretary of State (SoS) Brian Kemp on 10 May 2017 cites the security analysis of

Feldman, Halderman, and Felten. The GEMS central server software analysis by Ryan and Hoke, cited in the same letter, shows flaws in the central server. The fact that all analyses of the "standard" Diebold election system, even operated in intended conditions, have found major flaws should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.

13. Evidence indicates that the April 18 and June 20 Special Elections were conducted using a "non-standard" customized Diebold DRE voting system, with an unusual configuration, not tested by a federally accredited laboratory.

14. Even more alarming is the fact that the CES server containing crucial election programming files was known to be open to entry and manipulation in August 2016, and this glaring security problem had not been corrected even as late as March 1, 2017.

15. We must assume that the failure to secure the system and its data caused the already unreliable and unfit system unquestionably to be vulnerable to undetected attack. The system must be considered compromised and it is only prudent that the system must be considered to have been compromised from August 2016 through March 2017, and should not be used to conduct a public election.

16. It has been well-established in the computer security world that the Diebold election system, as configured for "standard" use, is unfit for use due to security and reliability concerns. In my letter/request to Secretary Kemp, serving as a technical advisor to the citizens of Georgia who had petitioned for the non-use of the Diebold

systems in the 20 June 2017 election, I asked for responses to the questions of security and reliability. If the standard system had been modified by CES, and that system had been re-certified, and one could rely upon the security credentials of the KSU CES, then one might have some limited confidence in the suitability of the Diebold system for use in elections in Georgia.

17. The response from Secretary Kemp has been tepid at best. His letter of June 5, 2017, does not address technical questions, and does not really address the questions posed by the electors of Georgia in their original request to him.

18. To be specific, the report of 18 April 2017, attached to Mr. Gay's email to Merle King, is damning in what it says and what it does not say. What we see as "successes" are only that the response to a security incident went well. This is essentially the statement that when law enforcement officials arrived at the barn, they found the door closed, and they found no horses inside the barn, but they had arrived quickly.

19. We see a number of issues in the 18 April 2017 report that indicate that the KSU CES security protocols were insufficient, and we find no commentary on any of those protocols that might have mitigated the damage.

20. I do not see that there are technical comments about successful, or positive, security measures that would have mitigated the potential damage done by the fact that the CES system was apparently open to attack for an extended period by any determined actor.

21. Indeed, the report can be read to suggest that the CES was not following some of the most basic security practices taught to all undergraduates in a computer

security course. Issues 1 and 8, under "Opportunities for Improvement", for example, cite a poor understanding of risk and of asset value on a main server and a failure to perform a security assessment. This apparent failure to know and to understand basic principles of security would not be inconsistent with Mr. Lamb's account that sensitive data was still openly available months after he had notified CES of this major security problem.

22. We come to the bottom line. We know, because it has been shown repeatedly, that the Diebold system as it is standardly configured, has major flaws. We would believe, based on our knowledge of process in Georgia, that it is the responsibility of the KSU CES to mitigate (or perhaps even remove?) these major flaws. But we do not see, in the report regarding the operational practices of the CES, that there is reason to believe that they have in fact mitigated the known flaws, produced a system that has been federally or state certified, and provided to the citizens of Georgia an election system in which they can be confident. For these reasons, the voting system in use cannot reasonably be approved as "safe and accurate for use" as required by Georgia statute.

23. For these reasons, I would argue that the Diebold system ought not be used in elections unless and until a complete security analysis has been performed on the software and hardware and a complete verification and integrity check has been made of the databases, including voter registration databases. Nor should the reported results generated by the system be relied on for a determination of the outcome of the June 20 special election.

24. I affirm that the foregoing is true and correct.

Duncan A Buell

DUNCAN BUELL Date

Sworn before me this 29th day of June, 2017, in Columbia, SC

Rebecca [illegible]
NOTARY PUBLIC